VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

# Absolvování individuální odborné praxe

# Individual Professional Practice in the Company

2020 Radek Lichnovský

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra telekomunikační techniky

# Zadání bakalářské práce

Student: **Radek Lichnovský**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2601R013 Telekomunikační technika

Téma: Absolvování individuální odborné praxe
Individual Professional Practice in the Company

Jazyk vypracování:

Zásady pro vypracování:

1. Student vykoná individuální praxi ve firmě: XEVOS Solutions s.r.o.
2. Struktura závěrečné zprávy:
a. Popis odborného zaměření firmy, u které student vykonal odbornou praxi a popis pracovního zařazení studenta
b. Seznam úkolů zadaných studentovi v průběhu odborné praxe s vyjádřením jejich časové náročnosti
c. Zvolený postup řešení zadaných úkolů
d. Teoretické a praktické znalosti a dovednosti získané v průběhu studia uplatněné studentem v průběhu odborné praxe
e. Znalosti či dovednosti scházející studentovi v průběhu odborné praxe
f. Dosažené výsledky v průběhu odborné praxe a její celkové zhodnocení

Seznam doporučené odborné literatury:

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Zdeňka Chmelíková, Ph.D.**

Konzultant bakalářské práce: Dalibor Vaněk

Datum zadání: 01.09.2019
Datum odevzdání: 30.04.2020

VYSOKÁ ŠKOLA BÁŇSKÁ-TECHNICKÁ UNIVERZITA * Fakulta elektrotechniky a informatiky * OSTRAVA * 1D16

prof. Ing. Miroslav Vozňák, Ph.D.
*vedoucí katedry*

prof. Ing. Pavel Brandštetter, CSc.
*děkan fakulty*

# Prohlášení studenta

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne: *30. dubna 2020*

Lichnovský
.....
podpis studenta

# Prohlášení zástupce spolupracující právnické nebo fyzické osoby

Souhlasím se zveřejněním této bakalářské práce dle požadavků čl. 26, odst. 9 Studijního a zkušebního řádu pro studium v bakalářských programech VŠB-TU Ostrava.

V Ostravě dne: *30. dubna 2020*

.....
podpis zástupce

Rád bych zde poděkoval firmě XEVOS Solutions s.r.o. za nabídku odborné praxe a také mým kolegům za odborný dohled a pomoc při řešení mé bakalářské praxe.

**Abstrakt**

Tato bakalářská práce popisuje mé působení ve firmě XEVOS Solutions s.r.o., kde jsem pracoval na pozici Network Engineer. Hlavní náplní praxe bylo navrhnutí a realizace vylepšení síťové infrastruktury této společnosti a také vypracování návrhu řešení pro další zákazníky. Práce je rozdělena do několika částí. První část obsahuje představení firmy a pracovní zařazení studenta. V druhé části se objevují různé zpracované úkoly, na kterých student při svém působení pracoval. Poslední část se věnuje shrnutí průběhu praxe a jaké měla pro studenta přínosy.

**Klíčová slova**: VLAN; 802.1x; firewall; switch, router; AP; Cisco Meraki; cloud; NAT

**Abstract**

This bachelor thesis describes the course of individual practice in the company XEVOS Solutions s.r.o. in which I was assigned as a Network Engineer. The main goal of my practice was the implementation of an improved network solution for the company and the creation of new solutions for their clients. The thesis is divided into several parts. The first part includes a description of the company and the student's job classification. The second part describes various given tasks that were assigned to the student. The last part is focused on summarizing the practice and how it improved student's overall expertise in the field.

**Keywords**: VLAN; 802.1x; firewall; switch, router; AP; Cisco Meraki; cloud, NAT

# Obsah

# Seznam použitých zkratek a symbolů

| | | |
|---|---|---|
| IT | – | Information Technology |
| OSI model | – | Open Systems Interconnection model |
| IP(v4) | – | Internet Protocol (version 4) |
| MAC | – | Media Access Control |
| L3 | – | Layer 3 |
| WAN | – | Wide Area Network |
| LAN | – | Local Area Network |
| VLAN | – | Virtual Local Area Network |
| ID | – | Identifier |
| DMZ | – | Demilitarized Zone |
| DHCP | – | Dynamic Host Configuration Protocol |
| VLSM | – | Variable Length Subnet Mask |
| CIDR | – | Classless Inter-Domain Routing |
| AP | – | Access Point |
| RADIUS | – | Remote Authentication Dial-In User Service |
| NAT | – | Network Address Translation |
| PAT | – | Port Address Translation |
| ACL | – | Access-Control List |
| HSRP | – | Hot Standby Router Protocol |
| VRRP | – | Virtual Router Redundancy Protocol |
| STP | – | Spanning Tree Protocol |
| FTP | – | File Transfer Protocol |
| UDP | – | User Datagram Protocol |
| NAS | – | Network-Attached Storage |
| POE | – | Power Over Ethernet |
| ISP | – | Internet Service Provider |
| UPS | – | Uninterruptible Power Supply |
| WPA | – | Wi-Fi Protected Access |
| (P)EAP | – | (Protected) Extensible Authentication Protocol |
| MSCHAPv2 | – | Microsoft Challenge-Handshake Authentication Protocol version 2 |
| EAP-TLS | – | Extensible Authentication Protocol-Transport Layer Security |
| Cisco ISE | – | Cisco Identity Services Engine |
| SSID | – | Service Set Identifier |
| TTL | – | Time To Live |
| DoS | – | Denial of Service |
| NPS | – | Network Policy Server |

# Seznam obrázků

# Seznam výpisů zdrojového kódu

# 1 Úvod

Tato práce se zabývá mým působením ve firmě XEVOS Solutions s.r.o v rámci odborné praxe bakalářského studia. Pro možnost praxe jsem se rozhodl hlavně z důvodu získání nových praktických zkušeností, ale také proto, že jsem na takovéto profesionální pozici ještě nepracoval. Práce ve firemním prostředí je velmi odlišná od prostředí školních laboratoří, především z důvodu mnoha faktorů, které mohou zasahovat do mnou řešeného problému.

V první části mé práce se zabývám představením firmy XEVOS Solutions s.r.o, jejím hlavní zaměření na trhu, podrobnějším popisem mého pracovního zařazení a také hlavními technologiemi, které jsem v průběhu praxe využíval. V další části se poté věnuji jednotlivým úkolům, které mi byly přiděleny, jejich řešením a přínosem po výsledné implementaci. Poslední kapitola je věnována celkovému souhrnu mého působení ve firmě, zhodnocení nových zkušeností a poznatků a ohlédnutí se za znalostmi získanými během studia, které mi pomohly při řešení různých problémů.

# 2 Představení odborného zaměření firmy na trhu

## 2.1 Vznik a zaměření firmy XEVOS Solutions s.r.o.

Firma vznikla v roce 2008 jako ryze český start-up zabývající se poskytováním služeb v širokém spektru informačních technologií od servisu a podpory, přes cloudová nebo síťová řešení, až po dodávky hardwarového a softwarového vybavení. Mezi primární aktivity společnosti patří IT podpora a servis, kde figuruje jako nezávislý partner. Tyto služby jsou poskytovány jak na pobočkách, tak i přímo na místě u klientů. Dále firma poskytuje serverovou či cloudovou správu klientských řešení pro domácnosti i velké firmy. Mezi tyto služby patří například správa Office 365, Azure Active Directory, nebo Cisco Meraki. [1]

## 2.2 Pracovní zařazení studenta

Během mého působení ve firmě jsem pracoval na pozici Network Engineer, ale při velkém vytížení kolegů jsem si také vyzkoušel práci u servisního technika či jako výpomoc při řešení problémů pro různé zákazníky.

Na začátku praxe jsem se seznamoval se zařízeními Cisco Meraki, které firma využívá pro správu síťové infrastruktury své i svých klientů, a se kterými jsem poté pracoval po celou dobu praxe. Dále jsem pracoval se systémem Helpdesk, který je využíván jako komunikační nástroj pro řešení různých problémů mezi firmou a klienty nebo s aplikací VirtualBox, kterou jsem používal pro práci s virtuálními zařízeními. Při menším pracovním vytížení jsem byl také k dispozici kolegům při plnění lehčích úkolů, které nespadaly do oblasti mého zaměření.

Během praxe jsem spolupracoval s dalšími kolegy v týmu, se kterými jsem konzultoval návrhy a řešil různé problémy, které se v průběhu naskytly.

# 3 Využívané technologie

Hlavní využívanou technologií byl pro mě produkt Meraki společnosti Cisco. Ten vytváří platformu pro jednoduchou a výkonnou správu síťových prvků jak pro malé podniky, tak globální společnosti. Dlouhodobým cílem vývoje této platformy je zjednodušení práce v oblasti síťových řešení z důvodu neustále narůstajících požadavků na ty, kteří se této problematice věnují [2]. Poskytuje síťovým správcům vzdálený přístup ke všem zařízením uvnitř spravované oblasti a díky cloudovému řešení také možnosti konfigurace sítí, které se mohou nacházet v odlehlých lokalitách, bez nutnosti fyzického zásahu. Pro konfiguraci klasických síťových zařízení jsem měl možnost využít buďto webového rozhraní nebo klasické příkazové řádky, která je součástí systému. Ve většině případů jsem využíval příkazové řádky, kdy konfigurace pomocí webového nastavení mi přišlo časově náročnější a méně intuitivní, než jsem byl dosavad zvyklý, hlavně díky mým předešlým zkušenostem.

Jako diagnostický a testovací nástroj mi velmi dobře posloužil další produkt společnosti Cisco – Packet Tracer. Tento simulační program je primárně určen pro studenty Cisco Networking Academy jako pomocník pro získání praktických zkušeností. Nástroj umožňuje studentům experimentovat s chováním jednotlivých sítí, kdy je možné nasimulovat různé případy chování a konfigurace. Využívá se především jako náhrada za fyzické vybavení, kdy umožňuje tvorbu sítí s velkým počtem zařízení a také jako platforma pro simulaci řešení daných problémů. Mé využití spočívalo především v možnosti simulace fyzického zapojení již existující sítě, kde jsem mohl testovat různá nastavení, aniž bych musel zasahovat do reálného chodu firmy.

Pro přístup k firemním serverům a ostatním vzdáleným zařízením jsem využíval protokolu společnosti Microsoft - Remote Desktop Protocol. Ten poskytuje uživateli grafické rozhraní vzdáleného zařízení pomocí síťového připojení. Zabezpečení tohoto protokolu se s jeho vývojem výrazně zlepšilo, avšak jeho využívání je stále považováno za možné bezpečností riziko [3]. Proto je doporučováno, při tomto způsobu administrace, nastavit uživatelům jen ta práva, která jsou nezbytná k dokončení daného úkolu.

Pro potřeby testování jsem využíval lokální virtualizace. V dnešní době velice razantně narůstající trend, který přináší při využití jednoho fyzického stroje možnost tvorby několika strojů virtuálních. Hlavním omezením ovšem nadále zůstávají parametry hardwaru, na kterém chceme tuto technologii využívat. V mém případě jsem zvolil nástroj VirtualBox, skrz který jsem měl možnost tvorby virtuálních operačních systémů. Tyto systémy se využívaly především k testovacím účelů, jelikož při nesprávném řešení či nepředvídatelným chybám je zde možnost virtuální stroj smazat a začít znovu nebo nahrát starší verzi. Tímto způsobem je možné velmi razantně snížit dopad nesprávného nastavení na fyzických zařízeních. Nevýhodou je uzavřenost takového systému v „ideálním“ světě, takže zde nelze s naprostou jistotou říci, zdali řešení bude funkční i při ostrém nasazení v reálných podmínkách provozu.

# 4 Úkoly řešené při vykonávání bakalářské praxe

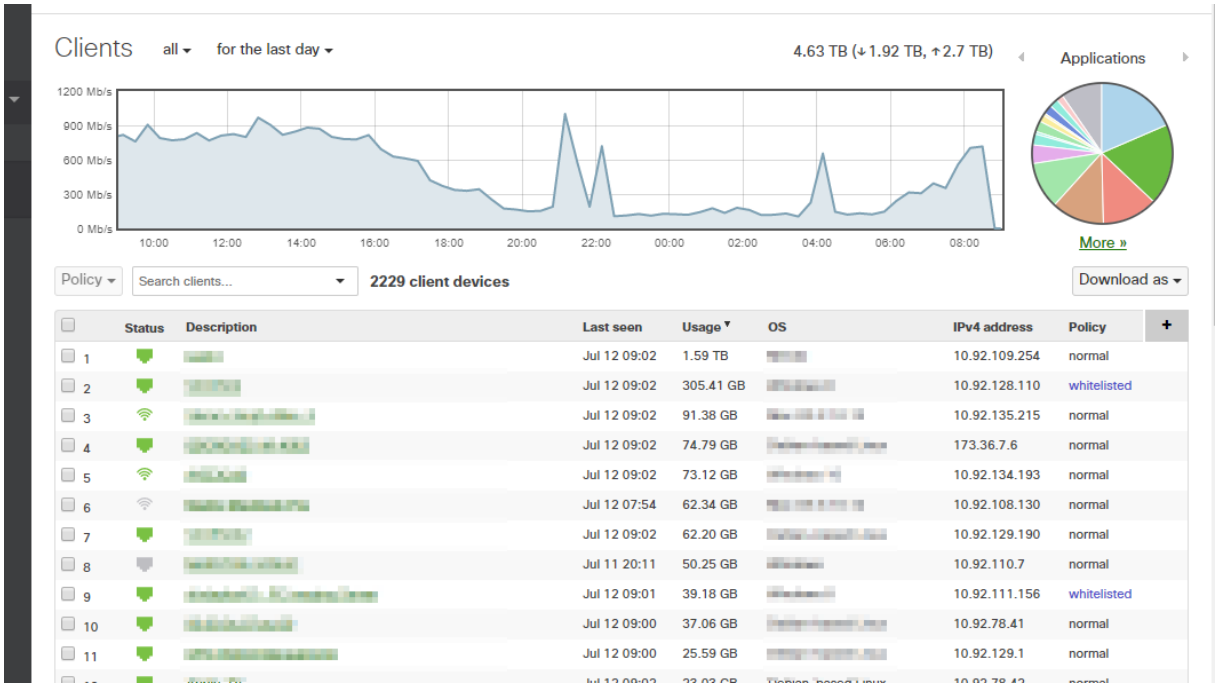
## 4.1 Seznámení se systémem práce ve firmě a využívanými systémy

Po mém nástupu do firmy bylo nutné, abych byl zaregistrován do všech potřebných systému a měl tak přístup do interní sítě. Prvním úkolem bylo seznámení se s využívanými technologiemi a také nastudovat fyzickou síťovou infrastrukturu, která je uvnitř firmy již zavedena. Při mé analýze síťového provozu jsem zjistil, že většina zařízení ve firmě fungují na bezdrátové síti Wi-Fi a bylo by tedy dobré zaměřit se především na její bezpečnost a dostupnost signálu. Pro koncové klienty je tato varianta připojení jedna z nejvýhodnějších z pohledu flexibility, ovšem pro síťového správce znamená nutnost mnohem většího ohledu na zabezpečení přenosu dat, kdy volba příliš slabého šifrování, či nízká komplexnost sdíleného hesla může vést až například ke krádeži firemních tajemství.

Už v této fázi jsem narazil na skutečnost, která mohla v budoucnu způsobovat problémy. Firma využívá ve své síti prvky různých značek a typů. To pro mě znamenalo nutnost nastudování konfiguračních procesů, které se od sebe mohou, i když ne příliš význačně, lišit. Zejména potřebné příkazy k nastavení jednotlivých funkcionalit. Tento fakt je způsoben tím, že každý výrobce implementuje systém ve svých zařízení trochu jiným způsobem. Většina ovšem stále vychází ze „standardu“, který zavedla společnost Cisco. Dále také tyto zařízení pocházely z různých produktových řad a podporovaly různé protokoly, nebo v opačném případě je nepodporovaly vůbec. Z tohoto důvodu nastal problém, kdy některá řešení, která by byla výhodná a také jednoduše implementovatelná, musela být zamítnuta.

Největším rozdílem oproti mým dřívějším zkušenostem bylo využití produktů z rodiny Cisco Meraki. Konfigurace těchto síťových prvků je již řešena skrze cloudový přístup, nikoli pomocí příkazové řádky, která se vyskytuje u klasických Cisco zařízení, a na kterou jsem byl v minulosti zvyklý. Tento přístup ovšem také znamenal různé výhody, zejména nebylo nutné vědět, kde se prvky fyzicky nacházejí nebo jaký je k nim přístup. Ve stejném čase zřejmou nevýhodou je nutnost připojení k internetu, kdy při jeho výpadku se tento způsob konfigurace stává nevyužitelným. V takovéto situaci je tedy u administrátora nadále kladen důraz na znalost příkazové řádky, kterou je stále možno skrze konzolový port nebo pomocí vzdáleného připojení využívat.

Mým prvním úkolem, sloužícím primárně jako možnost projít si celým systémem, byla kontrola konfigurace jednotlivých síťových prvků, zdali některá nastavení nejsou zbytečná nebo neomezují případnou možnost komunikace různých zařízení. Hlavním zaměřením pro mě bylo nastavení firewallu, kde jsem se zabýval zjednodušením či úpravou pravidel.




Obrázek 1: Webové rozhraní Cisco Meraki [4]

## 4.2 XEVOS Solutions s.r.o.

Navrhnout řešení pro zvýšení bezpečnosti bezdrátového připojení a oddělení síťového provozu uvnitř firmy s pomocí využití VLAN.

### 4.2.1 Počáteční stav a analýza zadání

Při mém nástupu již byla interní síť rozdělena do několika samostatných VLAN. Toto rozdělení ovšem bylo uděláno pouze jako dočasné a také se ukázalo jako možné bezpečnostní riziko, protože pouze základně oddělovalo adresní rozsahy pro DHCP, neřešilo ovšem omezení přístupu různých uživatelů. Z pohledu bezpečnosti, kdy všichni klienti byli připojování do stejného adresního rozsahu, se mohl prakticky kdokoliv dostat do jakékoliv části sítě. Samotné připojení k bezdrátové síti zabezpečeno bylo, ovšem pouze s použitím sdíleného klíče. Tato forma zabezpečení je na firemní úrovni v dnešní době již nedostatečná, protože při znalosti tohoto klíče je možné proniknout do interní sítě a bez zavedených dodatečných opatření získat přístup až ke kritickým či tajným informacím. I když je tato metoda zabezpečena šifrováním WPA2, hlavním faktorem stále zůstává člověk, a je tedy možné, že administrátor lehkomyslně využije snadno prolomitelného hesla nebo jej vyzradí zdánlivě důvěryhodné osobě.

Po seznámení se se síťovou infrastrukturou jsem si celou síť nasimuloval v nástroji Cisco Packet Tracer a zde také začal navrhovat další postupy. Prvním úkolem, ještě před zahájením konfigurace jednotlivých zařízení, bylo určení rozsahů IP adresování a jejich rozdělení do příslušných VLAN.

### 4.2.2 Návrh adresního rozsahu

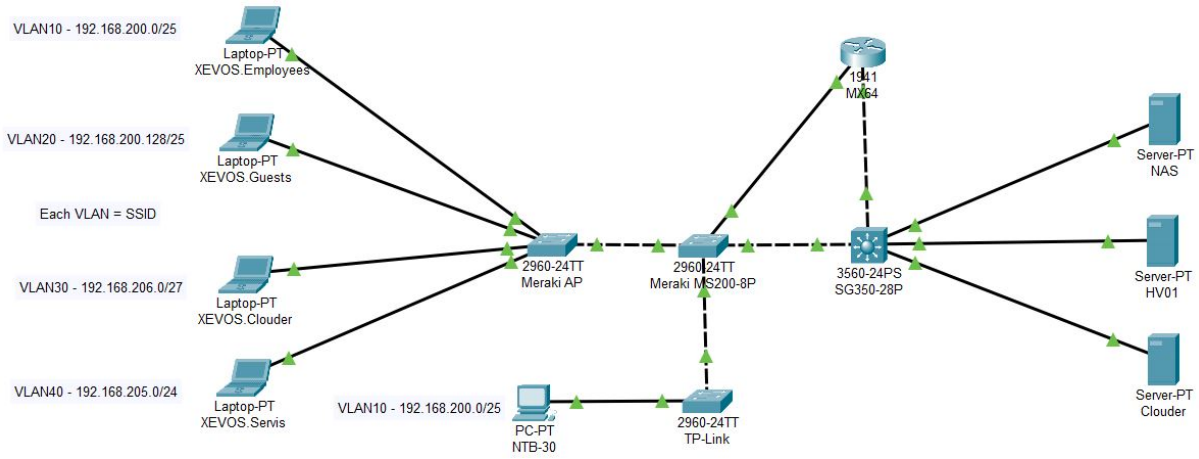
VLAN slouží pro logické rozdělení sítě nezávisle na fyzickém zapojení. Tento způsob rozdělení je prováděn na druhé vrstvě OSI modelu, nejčastěji s využitím switchů. Takto rozdělené sítě mezi sebou nesdílí adresní rozsah a každá tedy spadá do vlastní broadcastové domény. Využití této technologie napomáhá mimo jiné i ke snížení zatíženosti switche, kdy broadcastové rámce jsou distribuovány pouze uvnitř daných VLAN, nikoli do celé sítě. Zařízení, nacházející se uvnitř rozdílných VLAN, mezi sebou nedokážou komunikovat bez pomoci zařízení 3. vrstvy jako je například L3 switch nebo router. Oddělení provozu funguje na základě přidání tzv. tagů do přenášeného síťového rámce. Toto řešení umožňuje jeho separaci bez nutnosti nasazení více fyzických zařízení. Co se týče zabezpečení, samotné nasazení VLAN v síti by nemělo být bráno jako bezpečností opatření. V případě nesprávné konfigurace je možné síť napadnou pomocí různých útoků jako je např. VLAN Hopping Attack [5]. Většině těchto útoků se ovšem dá předejít správným nastavením switchů.

První překážkou byl požadavek firmy na co nejmenší zásahy do již fungujícího adresního schématu kvůli činnosti kritických serverů apod. Z tohoto důvodu jsem se snažil adresy, které již byly staticky přiděleny, obejít a ponechat beze změny i přes možné budoucí problémy jako je např. řízení přístupu, směrování nebo finální nesourodnost adresního schématu.

V dřívějších dobách se při tvorbě sítí využívalo tzv. classful adresování. Tento typ adresace rozděloval všechny dostupné adresy do 5 různých tříd. První 3 třídy se využívaly pro tvorbu samostatných sítí s ohledem na jejich velikost (třídy A - C). Další dvě třídy (D a E) byly rezervovány jako speciální adresy. Největším problémem, a také důvodem nahrazení tohoto způsobu rozdělení, byla velká nevyužitelnost adres z bloků A a B [6]. To vedlo k přechodu na classless adresování (CIDR), kde se rozdělení adres do jednotlivých tříd přestalo využívat.

S příchodem notace CIDR přišla možnost tvorby podsítí pomocí změny masky IP adresy. Podle velikosti masky určujeme počet adres, které je možné v dané podsíti uvnitř jednoho rozsahu alokovat.

Při tvorbě jsem vycházel ze standardního privátního rozsahu adres 192.168.0.0/16. Tento rozsah jsem rozdělil na různé podsítě, kde každá pokrývala jinou oblast využití např. jedna pro kamerový systém, další pro Wi-Fi síť návštěv firmy, zaměstnanců apod. Dalším krokem bylo rozhodnutí, zdali je nutné využít proměnlivých délek mask adres z důvodu omezení adresních rozsahů. Tento způsob tvorby sítí má odbornou zkratku VLSM. Můj první návrh tento princip využil, kdy jsem se snažil podle počtu zařízení udělat rozsahy co nejmenší. Nakonec se ale od tohoto návrhu upustilo z důvodu finální nepřehlednosti adresního schématu a také nízkého počtu VLAN, takže zde nefiguroval problém nedostatku IP adres. Hlavní oblastí využití tohoto způsobu dělení je především při tvorbě a rozdělování veřejných adresních rozsahů. Výsledná forma tedy využívala rozsahy s fixní maskou /24, které umožňují alokaci až 254 adres pro koncová zařízení.




Obrázek 2: Návrh sítě s využitím VLSM v programu Packet Tracer

### 4.2.3 Konfigurace síťových prvků

Po zvážení a schválení adresního rozsahu jsem přešel ke konfiguraci síťových prvků. Tyto prvky se v síti vyskytovaly v podobě 3 typů - switche, routery a access-pointy.

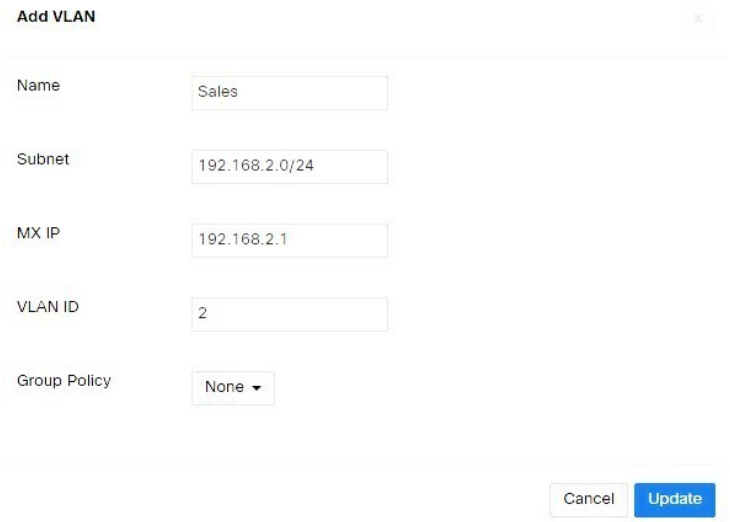
Switch je prvkem využívaným na 2. vrstvě síťového modelu OSI. Umí tedy pracovat pouze na úrovni fyzických adres (MAC adresy), nikoli na síťové vrstvě, která pro komunikaci využívá adres internetového protokolu (IP adresy). Switch se stal logickým nástupcem dříve využívaného hubu, kdy odstranil jeho praktickou nevýhodu, která veškerá přijatá data odesílala pomocí broadcastu všem připojeným zařízením. Switch již přijatá data na základě MAC adresy odesílá pouze tomu zařízení, které je cíleným příjemcem. Také vytváří na každém ze svých portů oddělenou kolizní doménu, čímž pomáhá ve většině případů eliminovat možnost kolize, která může nastat v případě, že se dvě zařízení snaží naráz vysílat ve stejnou dobu. Broadcastová doména je sdílena mezi všemi zařízeními ve switchi, pokud síť není rozdělena pomocí VLAN.

Uvnitř firmy se těchto switchů nacházelo více. První sloužil pouze pro připojení všech ethernetových zásuvek. Nebyla zde potřeba žádné speciální konfigurace, protože pouze sdružoval všechny zásuvky do jednoho prvku. V této chvíli jsem neřešil rozdělení sítě na úrovni metalického vedení, ale pouze s využitím Wi-Fi, takže nebylo nutné se zabývat tím, zdali by některé porty vedoucí k zásuvkám měly spadat do různých VLAN.

Druhým v pořadí byl switch Meraki. Zde se již využilo nastavení pomocí webového aplikace. Toto nastavení probíhá trochu jinak než při práci v klasické konzoli. Meraki sdružuje všechny síťové prvky, které spadají pod danou organizační skupinu, například firma, do jednoho uživatelského rozhraní, kde je možné konfigurovat všechna tato zařízení. Samotný průběh nastavení zůstává podobný, jako u klasických switchů, s tím rozdílem, že se zde neprovádí tvorba VLAN. Ta, společně s udáním adresních rozsahů, které budou pro jednotlivé VLANy dostupné, se provádí už při nastavování Meraki routerů. Při konfiguraci switche tedy zbývá pouze přiřazení VLAN na jednotlivé porty a uvést je do daného operačního režimu.

Porty switche je možné uvést do dvou režimů - access, trunk. Access porty přenáší komunikaci pouze dané VLANy, kterou jim nastavíme. Veškerý provoz, který není označen daným VLAN-ID je blokován. V základním nastavení tyto porty přenáší provoz pouze nativní VLANy (VLAN 1). Druhým typem jsou porty operující v režimu trunk. Tyto porty dokážou přenášet provoz více VLAN současně. Tato skutečnost může být velkou výhodou zejména pokud například ke komunikaci využíváme pouze jediného fyzického připojení. Pro identifikaci provozu switche využívají metody 802.1q, která jednotlivým síťovým rámcům přidává při průchodu zařízením VLAN-ID. V tomto případě, jak již jsem se zmínil v podkapitole 4.2.2, je nutné pro komunikaci mezi jednotlivými VLANy využít směrování. Většinu portů tohoto zařízení bylo nutné nastavit do režimu trunk z důvodu, že do něj přicházeli rámce z různých částí firemní sítě.

Meraki zařízení jsou vyvíjena s myšlenkou, že síť, ve které jsou využity, neobsahuje zařízení jiného výrobce. Tato skutečnost se odráží například při tvorbě VLAN, kdy, viz. Obrázek 3, je při konfiguraci nutné zadání i tzv. MX IP. Tento údaj je obdobou výchozí brány dané VLANy. Je to adresa rozhraní routeru Meraki, která jsou označovány jako MX.




Obrázek 3: Tvorba VLAN ve webovém rozhraní Meraki [7]

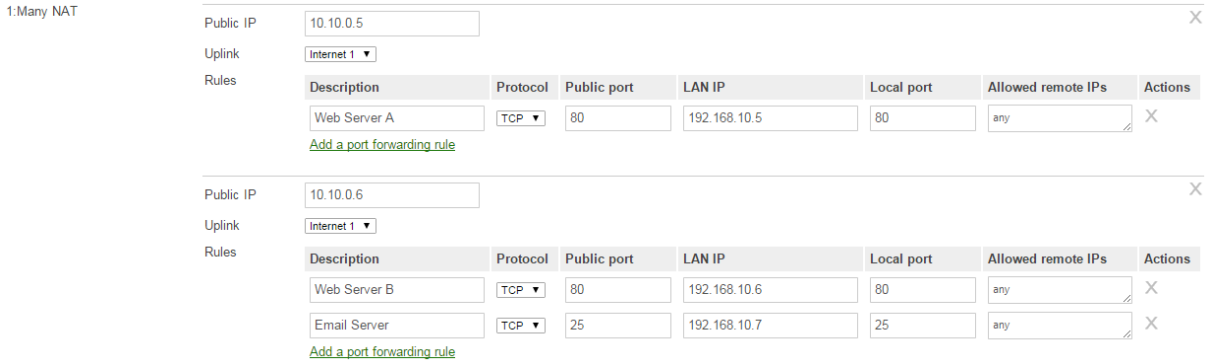
Do tohoto switche byly připojeny také všechny AP. V jejich nastavení můžeme změnit frekvenci na jaké budou vysílat (2.4 GHz, 5 GHz), zdali chceme zavést podporu různých protokolů nebo např. omezení jejich přenosové rychlosti. Z důvodu velkého využití Wi-Fi sítě zde bylo nutné si povšimnou, zdali v budově, kde se nacházíme, nedochází k příliš velkému rušení z důvodu využití stejných kanálů pro dané vysílací pásmo. S pomocí mobilní aplikace bylo zjištěno, že sítě vysílající na frekvenci 5 GHz, ovlivňovány nejsou. Ovšem většina sítí v pásmu 2,4 GHz vysílala na stejném kanálu. Tato skutečnost nemusí být v malé míře problémem, může ale vést ke snížení výkonnosti dané sítě nebo dokonce až k celkové nepoužitelnosti. Některá SSID tak byla přesunuta. Z důvodu rozdělení výkonu byla také pro vybraná SSID, například síť Guest, omezena operační rychlost.

Poslední switch se již řadil mezi vyšší řadu tzv. L3 switchů. Ty již mohou pracovat na 3. úrovni OSI modelu, což znamená, že jsme schopni využít různých síťových služeb jako např. směrování nebo DHCP. Tyto možnosti ovšem zatím zůstaly nevyužity, takže se zde nastavily pouze základní vlastnosti jako jsou VLANy a chování portů.

Posledním prvkem, který se stará např. o směrování, DHCP nebo poskytuje firewall, je hraniční Meraki router. Zde bylo nutné vytvořit požadované VLANy dle vypracovaného návrhu a nastavit rozsah adres pro každý VLAN tak, aby DHCP server věděl, které adresy smí využívat. Také se zde nastavily statické adresy pro zařízení, u kterých není žádoucí, aby se jejich adresa po uplynutí doby pro zapůjčení měnila. Dále bylo nutné nastavit pravidla firewallu, určující, která zařízení mají přístup do jednotlivých podsítí či přímo na daná zařízení. Jednou z mně dříve neznámých věcí, která zde byla využita, je tzv. demilitarizovaná zóna. Zařízení v této zóně mají striktně omezený přístup, a to pouze do internetu. Jakýkoli vstup do vnitřní části sítě (LAN) je jim zakázán. Toto pravidlo bylo využíváno zejména v oddělení zákaznického servisu, kde byla do sítě připojována cizí zařízení. Pro DMZ tak byla také vytvořena samostatná VLAN. V neposlední řadě zde bylo také nutné provést nastavení NAT.

NAT je metodou, která je využívána k překladu privátních adres na adresy veřejné. Tato technika byla vyvinuta primárně z důvodu rapidního čerpání veřejných IPv4 adres. Jeho hlavní výhodou je možnost překladu celých privátních rozsahů na jedinou veřejnou adresu registrovanou v internetu. Při základním rozdělení existují dva typy NAT - 1:1 a 1:N. První typ je využíván pouze pro překlad jedné privátní adresy na jednu veřejnou. V mém případě se využilo druhého typu, kdy bylo nutné za jednu veřejnou adresu schovat celou firmu. Všechny IP pakety směřující z privátní sítě mají pozměněnou svoji zdrojovou adresu na danou veřejnou. Při jejich návratu je po průchodu změněna jejich cílová adresa z veřejné zpět na privátní. Aby byl při komunikaci překlad adres jednoznačný, komunikačním protokolům jsou při navázání spojení pozměněny čísla portů. Pro tento způsob překladu se v dnešní době nejčastěji využívá termín PAT.

Nastavení NAT je při využití VLAN v nastavení Meraki automatické. Jedinou věcí, kterou bylo nutno nastavit bylo povolení přístupu k těm zařízením, které mají být viditelné z vnější sítě. Pro tento účel slouží metoda zvaná port forwarding. Pro jeho konfiguraci je nutno specifikovat vnější port, privátní adresu a lokální port serveru.




Obrázek 4: Nastavení port forwardingu v rozhraní Meraki [8]

### 4.2.4 Nastavení L3 směrování pro potřeby interní sítě

Dalším úkolem bylo nastavení směrování uvnitř společnosti z důvodu možnosti interní komunikace při výpadku hlavního routeru pomocí L3 switche. Tento typ switchů již disponuje využitelností funkcí 3. vrstvy OSI modelu. Hlavní rozdíl mezi tímto zařízením a klasickým routerem je ve způsobu rozhodování u směrování. Tradiční routery využívají pro své rozhodování mikroprocesorů, směrování je tedy řešeno softwarově. Naproti tomu L3 switche využívají hardwarového řešení s pomocí specializovaných modulů a pamětí [9]. Hlavním důvodem využití routingu již na switchi je snížení odezvy, kdy packet nemusí putovat až k routeru, kterému se tak současně i sníží vytíženost. Rozhodujícím parametrem je také celková výkonnost daného switche, který chceme pro tento účel využívat. Směrování se může uvnitř velkých sítí stát velmi náročným úkolem, který může vést k vyčerpání veškerého výkonu switche a vést tak ke zpomalení komunikace nebo přehřívání zařízení.

Tento úkol se nezdál příliš složitý, dokud po restartování switche nedošlo k úplnému odstřižení firmy od internetu a zamezení jakékoli komunikace a musela se nahrávat starší záloha. Po této zkušenosti jsem tedy začal s testováním na náhradním switchi stejného výrobce.

Switche využívané uvnitř firmy se řadí do řady „small-business“ od společnosti Cisco. Tato řada je navržena pro subjektivně jednodušší konfiguraci zejména pro menší firmy, které nemají specializované techniky, kteří by se zabývali hlubší problematikou síťové správy. Většinu potřebného nastavení je možné konfigurovat pomocí webového rozhraní, oproti klasickému přístupu přes konzoli. Připojení k rozhraní je možné přes tovární adresu nebo automaticky přidělenou adresu z DHCP. Osobně jsem si vybral cestu, která pro mě byla již známá, a to pomocí příkazové řádky. S tímto způsobem konfigurace jsem již měl zkušenosti a cítil jsem se mnohem jistěji.

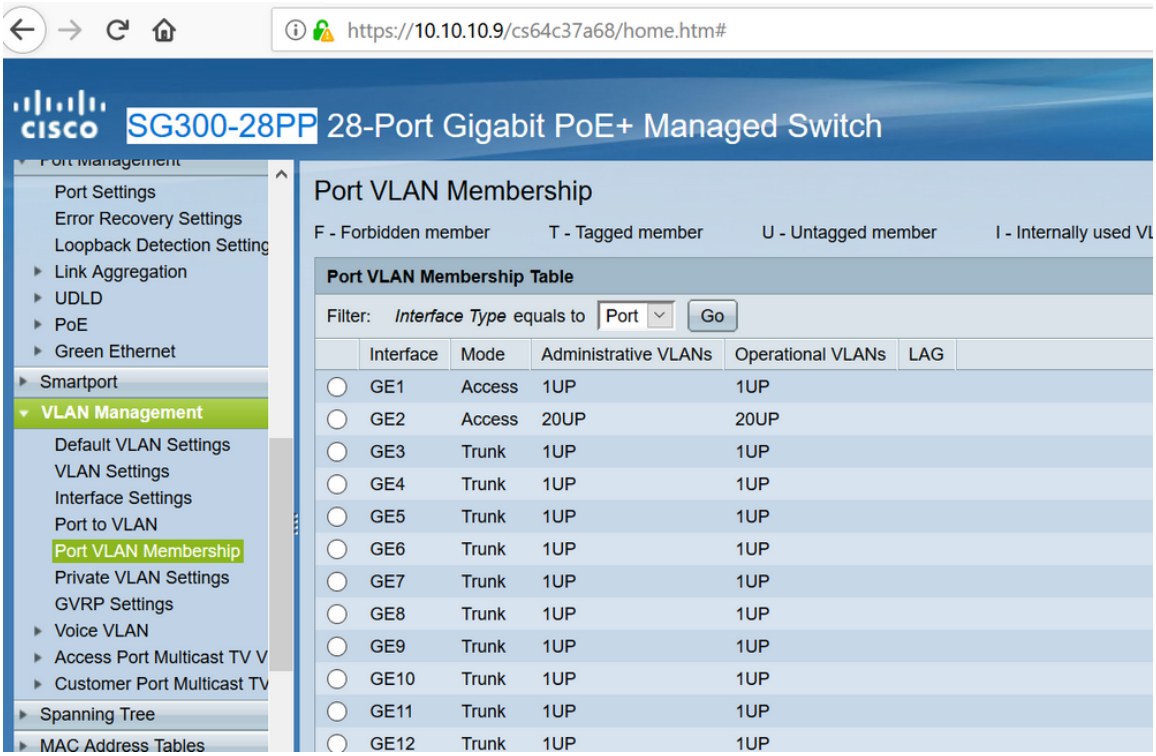
Nastavení spočívalo výhradně v ověření funkcionalit 3. vrstvy OSI, nadefinování rozsahů, které mají být v interním směrování zahrnuty, nastavení IP adres na dané rozhraní jednotlivých VLAN a nastavení portů do příslušných módů. Po ověření konfigurace byly do switche připojeny dva notebooky z odlišných podsítí, aby se otestovalo, zda směrování funguje v pořádku, což se ovšem znovu nepodařilo. Po několika továrních restartech na switchi, vymazání síťových

nastavení systému Windows, se jako naprosto triviální chyba ukázalo nastavení firewallu systému Windows, které blokovalo příchozí spojení a při jeho deaktivaci již směrování fungovalo bez větších problémů.

Dále bylo nutné vytvoření pravidel pro komunikaci s využitím ACL. Ty jsou v případě switchů využívány pro nastavení odchozích a příchozích pravidel síťové komunikace. Jedná se o bezestavovou filtraci, kdy switch pomocí pravidel kontroluje pouze jednotlivé packety a neuchovává si žádnou informaci o daném spojení. V případě komunikace je tedy nutné nastavit pravidla v obou směrech. Obdobou tohoto řešení je firewall. Jedná se již o stavovou filtraci, kdy je v paměti uchováván záznam o daném spojení. Tento způsob je využíván například u routerů. Při filtraci sleduje firewall celou konverzaci a také, zdali nepřichází packety, které nejsou součástí korektně navázaného spojení. Pro tvorbu ACL jsem využil již existujících pravidel, které byly nastaveny na hlavním routeru a odstranil ty, která se netýkala vnitřního provozu. Překvapením, alespoň pro mě, bylo, že při specifikaci portů v pravidlech jsou v této řadě zařízení využívány slovní názvy místo čísel portů, např. „www“ místo „80“. Čísla portů je možné využívat, ale bylo nutné tuto možnost v nastavení přímo specifikovat.

Poté nastal další problém týkající se výchozí brány. Tu bylo nutné, z důvodu nastavení L3 switche, přesunout pryč z routeru. Tato změna vedla ke zprovoznění interního směrování bez pomoci hlavního routeru, ale také k absolutní nemožnosti směrování směrem k hlavnímu routeru. Při bližším zkoumání jsem přišel na to, že Meraki zařízení nepracují na stejném principu jako klasická Cisco zařízení. Díky uzavřenému ekosystému, jehož součástí jsou zařízení Meraki, s nimi ostatní zařízení nedokážou komunikovat na příliš hluboké úrovni. Z tohoto důvodu nedokázal klasický switch rozeznávat různá MX rozhraní Meraki a nebylo tedy možné využití směrování jednotlivých VLAN. Samotná Meraki zařízení navíc nefungují na principu jednoduchého rozdělení, kdy je možné o daném zařízení říct, že je „čistě“ router. Tímto omezením odpadla možnost směrovat provoz z vnitřního L3 switche při použití více VLAN na hlavní router a tím pádem i celý plán na využití tohoto switche jakožto záložního směrovače.

Po konzultaci problému s kolegy se rozhodlo, že tato problematika bude v budoucnu nejspíše řešena přidání dalšího Meraki zařízení, které si s tímto problémem již dokáže poradit. Limitací zde byla především nesourodnost zařízení v síti.

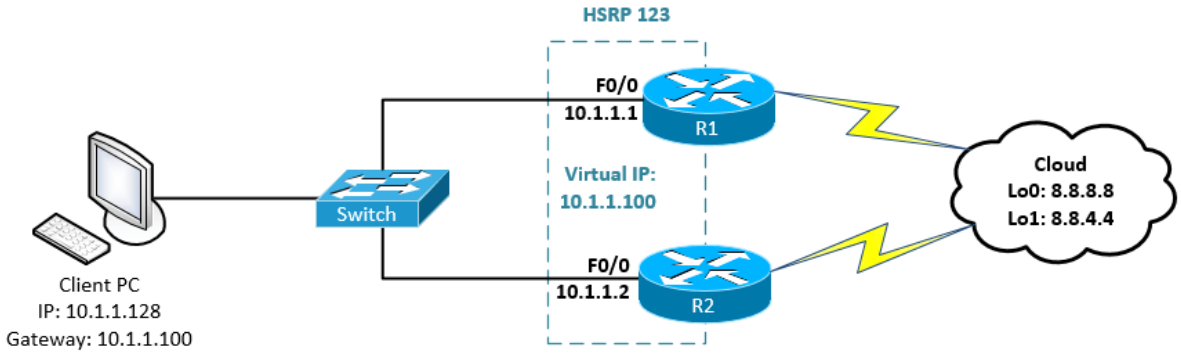



Obrázek 5: Webové rozhraní switche SG-300 [10]

### 4.2.5 Návrh řešení záložní cesty do internetu

Tento úkol spočíval v navržení řešení, které by poskytlo záložní cestu připojení do internetu v případě výpadku připojení k ISP. Již při prvním pohledu ovšem bylo zřejmé, že hlavním problémem je, že firma disponuje pouze jedním hlavním routerem, kdy jeho výpadek by znamenal úplné odstřižení jak firmy, tak i hostovaných služeb od internetu.

Tento problém jsem začal řešit jako první, protože výpadek samotného zařízení je více pravděpodobný a měl by větší dopad na celkovou komunikaci než možný chvilkový výpadek internetu. Řešením, kterým jsem se začal zabývat, bylo postavení firemního L3 switche na stejnou úroveň jako je hlavní router. Zde se naskytla možnost využití Cisco proprietárního protokolu HSRP. Tento protokol dovoluje nakonfigurovat více redundantních směrovačů, které existují v jedné síti. Při takovéto konfiguraci se směrovače začnou jevit v síti logicky jako jeden a je pro ně vytvořena jedna virtuální IP a MAC adresa. Všechen provoz je směrován skrze jeden směrovač v dané skupině, který byl protokolem určen jako primární. Jakmile se tento směrovač přestane hlásit, provoz je přesunut na záložní. Většinu času klient ani nepozná, že někde po cestě nastal problém. Pokud se spojení s primárním směrovačem obnoví, protokol automaticky přesměruje provoz nazpátek. Toto řešení bylo opět zprovozněno v simulačním prostředí. Ukázalo se ovšem, že i když jak L3 switch, tak Meraki router jsou dílem společnosti Cisco, Meraki tento protokol nepodporuje vůbec a daný switch, jak již jsem zmínil v podkapitole 4.2.4, není kategorie Enterprise, takže podporuje pouze otevřenou verzi tohoto protokolu zvanou VRRP.




Obrázek 6: Příklad chování routerů s využitím protokolu HSRP [11]

Z důvodu neúspěchu s HSRP jsem se tedy začal zabývat protokolem VRRP. Tento protokol vychází z principu HSRP s tím rozdílem, že není majetkem společnosti Cisco. I když jsou si tyto protokoly velmi blízké, a oba jsou využívány k dosažení stejného cíle, jejich vzájemná kompatibilita není možná. Tento pokus ovšem skončil stejně jako můj předchozí, protože při bližším studování zařízení Meraki jsem zjistil, že mají implementovanou vlastní verzi tohoto protokolu zvanou „Warm Spare“, která není kompatibilní s žádným z výše uvedených protokolů. Tento protokol má také své omezení, kdy jednotlivé Meraki zařízení musejí být stejného typu i série.

Posledním nepermanentním nápadem byla konfigurace více výchozích bran na koncových stanicích se vzájemným využití služby, která je zahrnuta v instalaci Windows, Dead Gateway Detection. Tato služba dokáže na klientské stanici detekovat výpadek výchozí brány a přesměrovat provoz skrze bránu záložní. Její nevýhoda ovšem spočívá, že při obnově spojení hlavní brány již nedokáže provoz přesměrovat nazpět, ale zanechá jej běžet skrze záložní bránu.

Jako dlouhodobé řešení jsem po konzultaci s kolegy navrhnul přidání nového zařízení Meraki, které by bylo spárováno s již existujícím.

Druhou částí problému byla skutečnost, kdy internetové spojení je do firmy poskytováno pouze pomocí jediného připojení k ISP. Tento problém byl nakonec dočasně vyřešen přidáním mobilního routeru s datovou kartou. Ten byl připojen do Meraki routeru, ve kterém je možno přímo nakonfigurovat jeden port jako záložní WAN připojení. V případě výpadku je tedy automaticky provoz přepojen na mobilní internet do doby, dokud se port s hlavním kabelovým připojením opět nepřihlásí.

Celkové řešení tedy spočívalo v pořízení nového routeru, nastaveného v režimu stand-by, který bude fungovat pouze jako záloha a zajištění internetového připojení pomocí druhého kabelu k jinému poskytovateli.

### 4.2.6 Autentizace uživatelů pomocí protokolu 802.1x

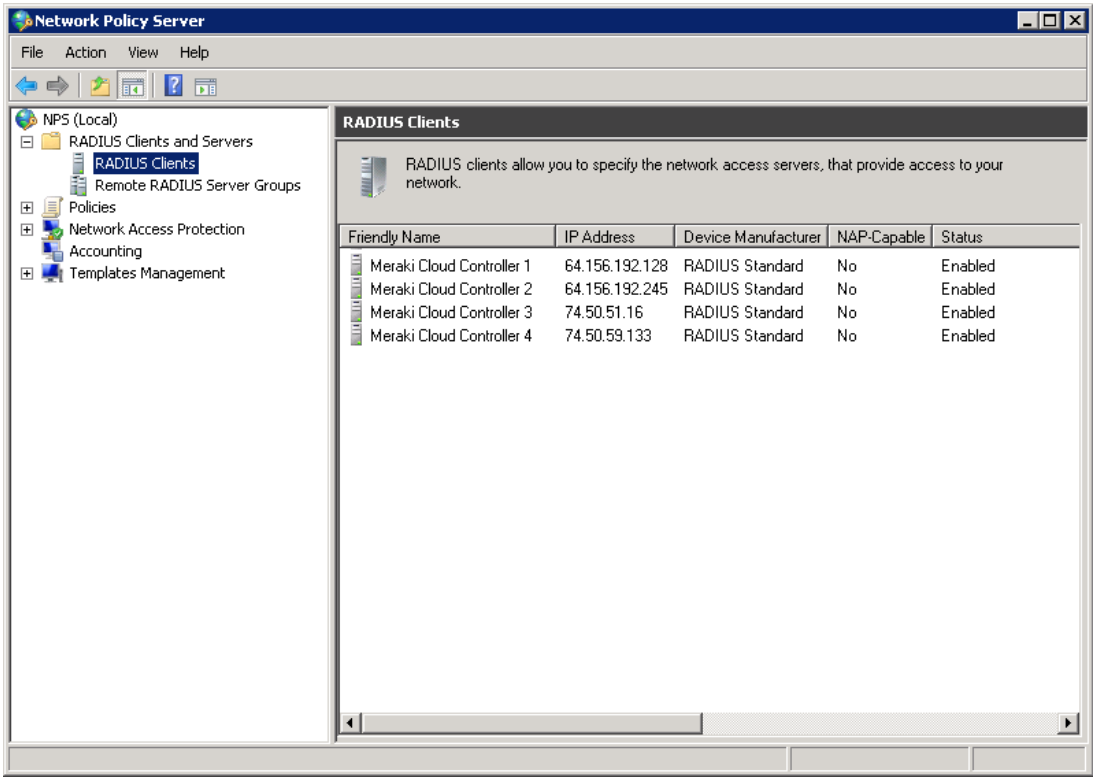
Dalším úkolem byla snaha o vylepšení zabezpečení bezdrátového provozu pomocí zavedení autentizace uživatelů s využitím technologie šifrování WPA2. Tento protokol se v dnešní době objevuje ve dvou formách, WPA2-Personal a WPA2-Enterprise. První typ je koncipován pouze pro využití v domácnostech, kdy autentizace neprobíhá pomocí 802.1x, ale pouze s pomocí sdíleného klíče. Tento typ zabezpečení byl využíván nyní. WPA2-Enterprise již využívá autentizace 802.1x a také poskytuje rozšířené možnosti zabezpečení, jako je např. dynamické přiřazování VLAN či možnost implementace pro kabelová připojení. Technologie obstará autentizaci uživatelů vůči určenému RADIUS serveru pomocí frameworku PEAP. Z důvodu nutnosti připojování mobilních a také různých cizích zařízení byla zvolena metoda autentizace pomocí jména hesla - MSCHAPv2. Za bezpečnější by se v dnešní době dala považovat metoda s využitím certifikátů EAP-TLS, kde však neustálá nutnost přenášení certifikátu představovala pro uživatele značnou míru nekomfortu. Roli zpracovatele požadavků v tomto případě hraje AP, který se stará o přeposílání autentizačních zpráv mezi serverem a uživatelem.

AP překládá požadavek na autentizaci do formátu zprávy „Access-Request“, která je odesílána na IP adresu RADIUS serveru skrze UDP port, který je určen v nastavení Meraki. Pro udělení oprávnění k přístupu uživatele musí AP obdržet od autentizačního serveru zprávu „Access-Accept“. V opačném případě je žádost zamítnuta. Z důvodu urychlení komunikace se požaduje za žádoucí, aby IP adresy RADIUS serveru i samotného AP byly ve stejné broadcastové doméně, aby nebylo nutné do komunikačního řetězce zapojovat např. firewall či směrování [12].

Prvním krokem bylo nastavení role Windows Serveru, který poslouží jako RADIUS server. Tato role se nazývá NPS. NPS umožňuje vytvoření a provoz přístupových politik pro žádosti a vyřizování autentizace. Tuto službu lze také nakonfigurovat pouze jako logovací nebo do stavu RADIUS Proxy, kdy se NPS stará pouze o přeposílání žádostí na jiný RADIUS server [13]. RADIUS potřebuje ke správné funkčnosti něco, vůči čemu může porovnávat údaje zadané klienty, kteří žádají o přístup do sítě. V mém případě fungoval jako databáze seznam firemních doménových účtů ve službě Active Directory. Pro zajištění přístupu NPS do Active Directory je nutné zde daný server zaregistrovat. Doménové účty jsou ve firmě využívány i k přihlášení k personálním počítačům, což je pro uživatele výhodné ve směru, kdy pro autentizaci využívají stejného přihlašovacího jména i hesla.

Meraki zařízení, koncipována s ohledem na zjednodušení nastavení síťových prvků, ale také bezpečnost, požadují, aby autentizační server obsahoval vlastní platný identifikační certifikát. Tento certifikát se dá získat buď vygenerováním či přiřazením certifikační autoritou. Jelikož server, na kterém bylo NPS implementováno nebyl nový, tento certifikát již byl přítomen a nebylo nutno se jím dále zaobírat.

Dalším krokem bylo přidání jednotlivých AP jako RADIUS klienti do NPS. Zde bylo nutné pouze získat IP adresy jednotlivých AP, které se nachází v rozhraní Meraki a přidat tyto záznamy do databáze.



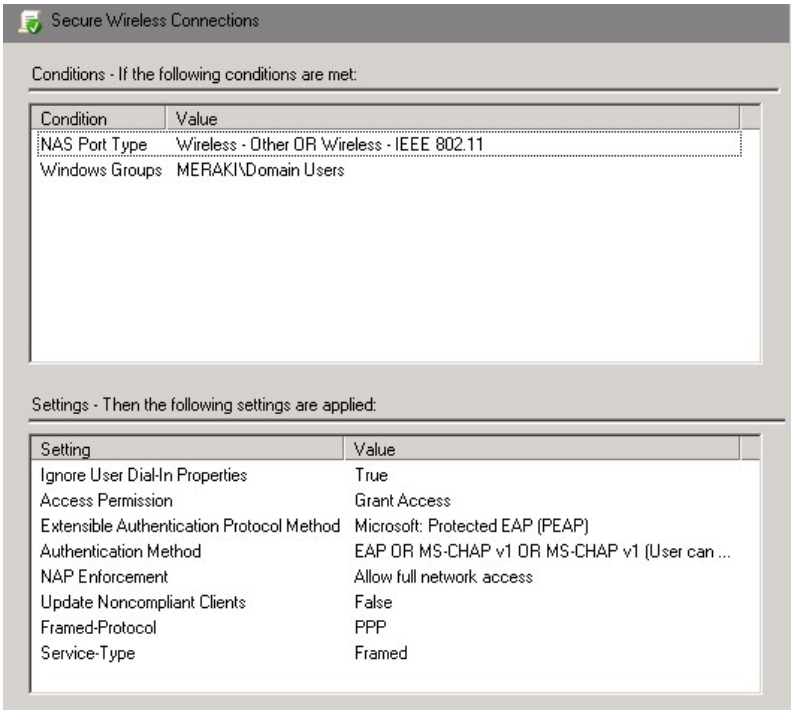

Obrázek 7: RADIUS klienti v NPS [14]

Dále bylo nutné nastavení tzv. politik pro umožnění podpory zvolené autentizační metody. Nastavení této politiky opět probíhalo za použití NPS. Při tvorbě bylo nutné nakonfigurovat specifické vlastnosti protokolu 802.1x. Pro autentizaci byla zvolena metoda PEAP. Tato metoda byla vytvořena jako bezpečnější varianta protokolu EAP, která poskytuje zabezpečení komunikace na transportní úrovni. Tuto metodu autentizace je možno využít, pokud chceme uživatele ověřovat pomocí uživatelských údajů či certifikátu. V mém případě je využíváno uživatelské databáze v rámci Active Directory, a tedy ověřování pomocí uživatelského jména a hesla. Tento typ autentizace využívá protokolu PEAP-MSCHAPv2. Jako poslední je nutné definovat doménovou skupinu uživatelů, vůči které budou údaje ověřovány.

S cílem tvorby co nejjednoduššího způsobu připojení k internetové síti je možné pro uživatele vytvořit politiku, která pro všechna koncová zařízení předdefinuje vlastnosti připojení. Tuto politiku je možné poté distribuovat pomocí doménového kontroléru všem počítačům.

Posledním krokem byla konfigurace nastavení zařízení Meraki. Zde byla potřeba jednotlivým SSID, která ve firmě existují, nastavit autentizační metodu WPA-2 Enterprise s využitím vlastního RADIUS serveru a přidání IP adresy, UDP portu a sdíleného klíče NPS.

Dalšími možnostmi autentizace je například pomocí MAC adres zařízení nebo pomocí využití služby Cisco ISE.




Obrázek 8: Příklad politiky NPS podporující PEAP-MSCHAPv2 [12]

### 4.2.7 Omezení přístupu uživatelů

Další věcí, kterou bylo nyní možno řešit díky RADIUS serveru bylo dynamické přiřazování jednotlivých uživatelů do daných VLAN ihned po jejich autentizaci. Díky NPS je možné vytvoření politik určují pravidla chování v síti, které se aplikují pro danou skupinu či uživatele. Tyto politiky obsahují také údaj, který přiřadí VLAN-ID danému uživateli. Po úspěšné autentizaci vůči RADIUS serveru je tato informace odeslána ve zprávě Access-Accept jako atribut Tunnel-Private-Group-ID. Pro zajištění funkčnosti je nutné systému Meraki nastavit, aby tento atribut využil při jeho obdržení. Ve výchozím nastavení přiřazuje VLAN-ID samotné Meraki a nebere tento atribut RADIUS serveru v potaz [12]. Dynamické rozdělování uživatelů napomáhá k vyšší bezpečnosti a kontrole v síti, kdy každý nově připojený uživatel je ihned zařazen tam, kde má být. Nemůže se tedy stát, aby např. firemní návštěva získala přístup ke zdrojům vývojářského týmu.

Pro tento úkol jsem vypracoval pouze vypracoval návrh a podrobnější dokumentaci, protože mi bylo řečeno, že v blízké budoucnosti budou ještě v síti probíhat výraznější změny, takže se tento problém bude dále řešit až později.

## 4.3 Firemní zákazník

Analýza a návrh řešení adresace společnosti a úprava hardwaru.

### 4.3.1 Počáteční stav a analýza zadání

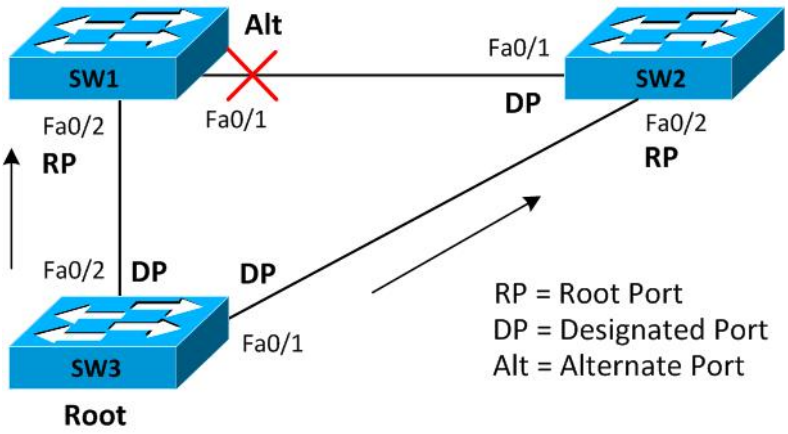
Tato firma je zákazníkem firmy XEVOS Solutions s.r.o., která je v procesu stěhování do nové lokality. Z tohoto důvodu zde byla síť vybudována pouze s ohledem na funkčnost bez jakéhokoli dodatečného hlubšího nastavení. Mým hlavním úkolem zde bylo navrhnout budoucí řešení v oblasti adresního rozložení, dokumentace a evaluace použitých síťových zařízení a úprava fyzického zapojení těchto zařízení.

### 4.3.2 Úprava kabeláže

Prvním úkolem bylo upravení fyzického zapojení z důvodu velmi obtížnému přístupu k síťovým prvkům a ostatním zařízením. Veškeré úpravy se prováděli za plného provozu, což znamenalo vysoké nároky na co nejrychlejší změny z důvodu zajištění přístupnosti sítě. Při propojování různých typů zařízení je nutné brát ohled na typ kabeláže, která je k propojení určena. Propoje jsou realizovány pomocí dvou typů kabelů - přímé a kroucené. Přímé kabely jsou nejrozšířenějším typem, jež jsou využívány například k propojení personálních počítačů se switchi nebo domácími routery. Kroucené kabely jsou méně běžným typem a jsou využívány k propojení stejných typů zařízení jako jsou například dva počítače. V dnešní době již toto rozdělení nehraje příliš vysokou roli, kdy novější zařízení již dokáží i při použití špatného typu kabelu komunikaci úspěšně navázat a udržet. Na druhou stranu z důvodu stále velkého využití starších zařízení uvnitř např. menších firem je stále dobré věnovat tomuto faktu pozornost. Při úpravách bylo nutné brát ohled i na to, že některé porty switchů byly tzv. POE neboli porty, které mohou připojeným zařízením kromě samotné komunikace poskytovat také elektrickou energii. Do těchto portů byly výhradně zapojeny především bezpečnostní kamery. Dále bylo zjištěno, že některé linky tvořily uzle uvnitř sítě. Tento problém nebyl dříve zjištěn z důvodu automatického řešení pomocí protokolu STP, který vybrané porty blokoval.

Protokol STP se stará o vytvoření logické topologie, ve které se nenachází žádné smyčky, které mohou vést k vytvoření tzv. broadcastových bouří. Tyto bouře jsou způsobeny faktem, kdy je ve smyčce zacyklen broadcastový provoz. Díky skutečnosti, že hlavička 2. vrstvy OSI nepodporuje hodnotu TTL, vysílané rámce se ze sítě nikdy neztratí. Umělé vyvolání těchto bouří je také někdy využíváno jako forma DoS útoku.

Po úpravě a výměně některých kabelových spojů se všechny, z důvodu přehlednosti, označily příslušnými štítky a byly zavedeny do kolejnic po stranách racku. Posledním úkolem bylo odstranění internetových kabelů, které vedly skrze prostor po snížení stropu do dalších pater.




Obrázek 9: Spanning Tree Protocol [15]

### 4.3.3 Přidání záložních zdrojů napájení

Na přání zákazníka byly zakoupeny 2 nové UPS, které slouží jako dočasná záloha napájení, pokud dojde k výpadku proudu. Tyto UPS bylo nutné zapojit do různých okruhů v budově, kdy každé patro je připojeno k jinému rozvaděči a v minulosti byly výpadky pouze částečné, nikoli v celé budově. Pro potřeby zapojení do elektrické sítě bylo nutné vytvořit třífázové zásuvky.

Do UPS byly poté připojeny důležité firemní servery, aby bylo možné přejít k jejich korektnímu vypnutí v případě výpadku energie. Konfigurace těchto záložních zdrojů probíhala automaticky po připojení do sítě, pouze bylo nutné nastavení jejich adres na statické z důvodu přehlednosti a správy.

### 4.3.4 Tvorba adresního schématu

Při analýze sítě jsem zjistil, že její rozdělení bylo provedeno pouze pro oddělení hlavního provozu od komunikace bezpečnostních kamer. S rozsahem určeným kamerám bylo doporučeno nehýbat z důvodu, že jejich případná nefunkčnost by mohla znamenat velké bezpečností riziko. Druhý rozsah, který byl určen všem ostatním zařízením, a přidělován pomocí DHCP, jsem tedy poté rozdělil do několika VLAN, které pokrývaly dané oblasti uvnitř firmy.

## 4.4 Ostatní úlohy

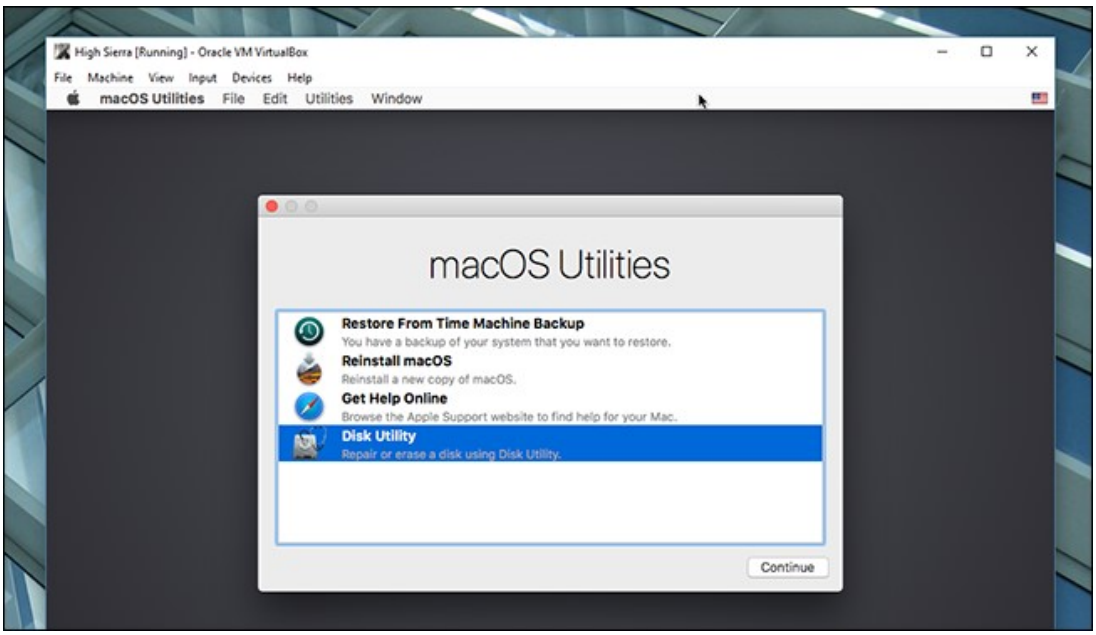
Z důvodu podstaty mé práce, kdy nasazení některých postupů mohlo být podmíněno prací jiného z mých kolegů či možnou delší dobou schválení nebo testování jsem při svém působení byl k dispozici také jako výpomoc při řešení problémů pro zákazníky firmy. Jednalo se o řešení problémů skrze firemní Helpdesk a manuální výpomoc pro servisního technika. Tyto problémy, především servisní, nesouvisely přímo s mým zaměřením, ovšem rád jsem se přiučil některým dovednostem, které jsou spojeny s hardwarovou stránkou IT.

### 4.4.1 Virtuální zařízení s prostředím macOS

Pro potřeby testování jistých prostředků a služeb, které firma nabízí či má ve své správě, mi byl přidělen úkol zprovoznění virtuálního počítače se systémem macOS, jehož virtuální disk byl poté uložen na firemní NAS. Hlavním důvodem byla především možnost testovacího prostředí pro řešení problémů, jejichž řešení bylo již zdokumentováno na platformě Windows, ale ne v systému macOS. Díky tomuto řešení bylo také možno předejít různým problémům např. s kompatibilitou či spoluprací různých služeb, které mohou být nasazeny ve stejném čase, ještě před jejich ostrým spuštěním v provozu.

Pro vytvoření jsem si vybral nástroj VirtualBox z důvodu předešlých, i když ne hlubokých, zkušeností. VirtualBox, existující jak ve 32, tak 64 bitové verzi, je virtualizační program pro široké spektrum využití, který spadá pod licenci GNU GPL jako open source produkt. Tento nástroj je komunitně vyvíjený s podporou společnosti Oracle, která se stará o splnění profesionálních kritérií [16].

Jako distribuci macOS jsem vybral nejnovější aktualizaci verze systému High Sierra. Novější distribuce jako je Mojave nebo Catalina jsou již dostupné veřejnosti, ovšem při jejich instalaci jsem se setkal s různými problémy jako jsou chyby instalačního balíčku nebo potíže se stabilitou systému. Po instalaci a otestování systému byla kopie virtuálního disku uložena na síťové úložiště, odkud bude později uvedena do provozu na jednom z firemních serverů jako virtuální zařízení.




Obrázek 10: Instalace macOS pomocí VirtualBox [17]

### 4.4.2 SPAM filtr emailové komunikace

Po více přijatých stížnostech, ať už firemních, či zákaznických, byl odhalen problém s filtrováním zpráv firemní komunikace. Byl jsem pověřen zjištěním příčiny a případným řešením tohoto problému.

Veškerá emailová komunikace ve firmě funguje na platformě Microsoft Exchange. Po udělení potřebných oprávnění k přístupu jsem začal hledat problém v administrátorské konzoli, kde jsem žádný zjevný problém nenašel. Přešel jsem tedy ke zpracování detailního výpisu emailů, které byly označeny jako SPAM a zjistil, že neexistovalo žádné pevné pravidlo, které by mělo za následek takovéto chování. Falešně označené zprávy byly od automatických systémových hlášení až po obchodní komunikaci, v jakoukoli denní dobu a náhodném množství.

Poslední možností bylo prohledání hlaviček špatně označených emailů a nalezení příznaků, které způsobovali toto chování. Nakonec jsem zjistil, že emaily jsou označovány automatickým filtrem, který využívá samotný emailový server.

Tento problém byl tedy nakonec předán k řešení společnosti Microsoft.

### 4.4.3 Script pro automatickou synchronizaci složky

Byl jsem požádán o vytvoření scriptu, který by po spuštění v daný čas automaticky synchronizoval danou složku ze serveru připojeného pomocí FTP s lokálně uloženou složkou. Script využíval pro synchronizaci programu WinSCP, což je volně dostupný open source FTP klient.

Pro synchronizaci bylo důležité, aby bylo scriptu umožněno pracovat bez nutného zásahu člověka. Vytvořil jsem si tedy seznam požadavků a začal studovat programovou dokumentaci WinSCP.

- Automatické řešení vyskakovacích oken během synchronizace
- Povolení možnosti přepisování již existujících souborů se stejným názvem
- Ukončení scriptu v případě chyby při přenosu
- Periodické spouštění scriptu v daném čase

Bylo nutné zjistit, zdali je ve scriptu možné zajistit automatické odpovídání na otázky, které v normální situaci vyžadují zásah uživatele. Pro tento případ jsem využil parametru *option*, který nám umožňuje např. automatické obnovení spojení, kdyby při přenosu dat došlo k jeho přerušení nebo ukončení scriptu, pokud se při spojení naskytne neočekávaná chyba [18]. Druhým typem otázky, která může vyvstat při přenosu souborů je, zdali chceme již dostupné lokální soubory přepsat. Tato možnost je také řešena v parametru *option* [18].

Aby byl scriptu umožněn přístup na FTP server, bylo nutné nejprve zajistit otisk klíče, který je poskytován serverem. Tento otisk je později využit k ověření totožnosti serveru. Pro otevření spojení jsem využil parametru *open*, kterému je nutno poskytnou základní informace o spojení jako je např. adresa serveru, uživatelské jméno a heslo a také dříve zjištěný otisk klíče [18].

Pro samotnou synchronizaci jsem využil scriptovacího příkazu *synchronize* s parametrem *local*. Tento parametr určuje, zdali chceme synchronizovat soubory z/do vzdáleného uložiště [18].

```
# Soubor SyncFiles.txt
option batch abort # Automatické odpovídání
option confirm off # Zrušení vyskakovacích oken s potvrzením
open ftp://username:password@server_add -hostkey="server_key_fingerprint" #
    Otevření spojení
synchronize local local_dir remote_dir # Synchronizace
exit # Ukončení spojení
```

Výpis 1: Synchronizační script pro WinSCP

Po vytvoření scriptu bylo nutné zajistit jeho spouštění v daném čase. Script jsem uložil do instalační složky WinSCP, kde jsem vytvořil **.bat* soubor, který script spouštěl.

```
winscp.com /script=SyncFiles.txt
```

Výpis 2: Obsah .bat souboru pro spuštění scriptu

Celý proces probíhal v prostředí Windows Server, takže pro spouštění scriptu v daném čase jsem využil implementovaného plánovače úloh ze systému Windows. Zde stačilo pouze nastavit dobu, kdy se má script spouštět.

### 4.4.4 Testování streamovací aplikace

Pro firmu je vyvíjena streamovací aplikace, která má za úkol pomocí Wi-Fi připojení přenášet v reálném čase obraz a zvuk vzdálené plochy. Celá aplikace má běžet na zařízení Raspberry Pi se systémem Raspbian, kde využívá multimediální framework FFmpeg. Pro samotné přehrávání byl zvolen přehrávač, který je dostupný současně se stažením frameworku, FFplay. Protože je Raspbian založen na Debianu, začal jsem se více zabývat problematikou Linuxového terminálu.

Aplikace je vyvíjena externím developerem, takže mým úkolem bylo testování jednotlivých buildů a zpětná vazba s nalezenými chybami nebo chybějícími funkcemi.

Při prvotním testování jsem odhalil nekompatibilitu aplikace s jiným rozlišením nežli nativním pro danou vzdálenou plochu, kdy po spuštění aplikace s chybou spadla. Dále se naskytl problém s odezvou, kdy rychlé přechody obrazovky nebo vykreslování komplexnějších snímků způsobovalo graduální zvyšování odezvy aplikace. FFplay podporuje při startu parametr pro benchmark přenosu, který byl použit pro zjištění, zdali zpomalování aplikace není způsobeno příliš velkým zatížení sítě, a tedy nedostatečnou rychlostí přenosu. Díky velké transparentnosti a otevřenosti, kterou poskytuje Linux, bylo pozorování využívaných prostředků jak zařízení Raspberry, tak sítě celkově jednoduché. Tento problém se ovšem nepotvrdil, takže všechny informace o chybách byly odeslány zpět k vývojáři.

Nová verze přinesla změny, které první testování téměř plně znehodnotily. Největší změnou byl přechod na nový typ video kodeku z H.264 na H.265, což znamenalo nutnost navýšení kapacity některých parametrů streamu a změnu formátu přenášeného obrazu. V této verzi byla také odstraněna možnost změny rozlišení obrazu, která byla nyní zafixována na 1080p. Při testování se ukázalo, že dochází k fragmentování obrazu a odezva se opět v průběhu času zvyšovala. Při spuštění benchmarku se ukázalo, že provoz vytvářený aplikací zahlcovat celé dostupné síťové pásmo, které bylo dispozici. Tento problém byl způsoben tím, že aplikace vykreslovala a přenášela při každém snímku celou obrazovku, nikoliv pouze dané části, kde došlo ke změně obrazu. Poslední nová verze, se kterou jsem měl možnost pracovat, již využívala interakce s rozhraním pro serverovou i klientskou stranu, takže pro mě odpadla možnost využití diagnostických nástrojů, které poskytoval FFplay při spuštění skrze příkazovou řádku.

# 5 Teoretické a praktické znalosti a dovednosti získané v průběhu studia uplatněné studentem v průběhu odborné praxe

V průběhu mojí praxe jsem se setkal s různými technologiemi. S některými jsem se již seznámil v průběhu studia, některé pro mě byly úplně nové. I když mi bylo jasné, že většina problémů, které jsou řešeny v laboratorním prostředí, ať už ve škole či různými simulacemi, neodráží situace, které mohou nastat v reálném nasazení, znalosti především z předmětu Počítačové sítě mi pomohly tím, že je pouze stačilo poupravit a aplikovat pro nasazení v daném systému. Další výhodou byly více teoretické znalosti z předmětu Telekomunikační sítě, díky kterému jsem získal hlubší porozumění o OSI modelu a jeho funkčnosti.

Při řešení některých problému, zejména týkajících se webové komunikace, byl pro mě také přínosný předmět Vývoj internetových aplikací, kdy jsem byl schopen pomocí různých nástrojů hledat problémy a neměl jsem problém orientovat se ve webových jazycích, i když jsem je využíval většinou pouze k diagnostice, nikoliv tvorbě nového obsahu. Tento předmět je volitelný a spadá pod katedru informatiky, ovšem v dnešní době internetu si myslím, že základní ponětí o této problematice může být velmi přínosné, což se v mém případě prokázalo.

Další výhodou pro mě byla znalost základních příkazů a pohybu v systémech Linux. Při mé práci jsem narazil na některé úlohy, které vyžadovaly využití tohoto systému a díky předmětům, které jsou ve valné většiny vyučovány právě s využitím Linuxu, jsem neměl větší problém při jejich plnění.

Největším přínosem za mé studium považuji 3. ročník, kdy se většina předmětů věnovala problematice, která mi již byla bližší. Samozřejmě celé bakalářské studium se nezabývá pouze oblastí síťařiny, a tak si myslím, že i ostatní předměty ať už elektrotechnické, či programátorské pro mě budou přínosné v dlouhodobém měřítku, protože je dobré mít alespoň základní rozhled v ostatních odvětvích IT.

# 6 Znalosti či dovednosti scházející studentovi v průběhu odborné praxe

Největším nedostatkem se pro mě ukázala ne moc hluboká znalost správy systému Windows Server. Především s tvorbou RADIUS serveru a službami s ním spojenými jsem si musel vypomáhat různými internetovými zdroji. Předmět zabývající se touto problematikou je možné si zvolit v letním semestru 3. ročníku, což jsem já neudělal. Myslím si, že co se týče síťové správy by tento předmět mohl být velmi přínosný. Také bych ocenil větší integrace zaměření, které se zabývá správou linuxových serverových systémů, protože jejich využití v profesionální sféře je velmi znatelné, a i když jsem se s nimi já osobně nesetkal, většina mých kolegů s nimi ne jednou musela pracovat.

Další nevýhodou pro mě byla celková neznalost systému Meraki. Ovšem tento nedostatek vyvstal zejména díky nezkušenosti s uživatelským rozhraním nežli kvůli chybějícím znalostem. Je jasné, že při výuce v bakalářských programech, které nejsou zaměřeny přímo na oblast síťařiny, není příliš praktické využití těchto zařízení s cloudovou správou z důvodu výuky pouze základních konfiguračních procesů. Na druhou stranu míti k dispozici pár takovýchto např. Meraki zařízení se mi zdá jako dobrá ukázka pro budoucí studenty.

Také bych ocenil, kdyby se při výuce, např. Počítačových sítí, více soustředilo na trend bezdrátových technologií. Při mém působení na praxi jsem měl možnost se podívat do firem, kde většina zařízení funguje pouze pomocí sítě Wi-Fi. Tato forma připojení koncových zařízení je dle mého názoru stále více populární, a i když si myslím, že připojení např. k ISP je stále nejlepší pomocí fyzického vedení, tak uvnitř menších prostor jako jsou firmy se bude bezdrátového připojení využívat stále více. Především, když už i většina základních desek stolních počítačů je vybavena Wi-Fi moduly.

# 7 Závěr

Možnost tvorby bakalářské práce formou odborné praxe hodnotím velmi přínosně. Tato možnost mě zaujala z důvodu možnosti vyzkoušení si práce v kolektivu a také řešení různých úkolů, které se mohou při správě reálně nasazeného systému vyskytnout. Možnost práce s technologiemi jako je např. Meraki mi umožnilo nahlédnout do oblasti cloudových řešení, která jsou, dle mého názoru, budoucností v různých oblastech informatiky. Při řešení síťových problémů jsem měl také možnost se naučit některé postupy a také čemu se vyvarovat při fyzickém návrhu a stavbě sítě jako byla například různorodost síťových prvků.

Oceňuji, že jsem měl možnost pracovat na různých úkolech, které se přímo netýkaly mého zaměření. Při výpomoci na servisu jsem měl možnost se seznámit s různými postupy práce, které se aplikují při manipulaci se zařízeními zákazníků nebo vyzkoušet si práci s různými typy zařízení, které se v rámci IT využívají. Při mé práci na Helpdesku jsem se také dozvěděl, že větší množství věcí, které pokládám za celkově jednoduché či v dnešní době již samozřejmé je pro většinu lidí stále velkou neznámou.

Také jsem zjistil, že většina problémů, které vyvstanou při chodu i např. menších sítí, je dobré řešit ihned, a i sebemenší problém stavět na stejnou úroveň jako ty zdánlivě kritičtější, protože v konečném důsledku mohou nadělat více škod, než se může na první pohled zdát.

Co se týče tématu, které jsem zvolil, tak mě tato zkušenost přivedla k závěrům, že bych se i nadále chtěl tomuto odvětví věnovat, a především se zaměřit na kybernetickou bezpečnost, na kterou jsou v dnešní době stále větší nároky. I z tohoto důvodu jsem se rozhodl pokračovat na magisterském studiu právě v oblasti bezpečnosti.

# Literatura


1. *O nás | XEVOS*. XEVOS Solutions s.r.o., 2020. Dostupné také z: https://www.xevos.eu/o-nas/.
2. *Cisco Meraki | About Meraki*. Cisco Systems, Inc., 2020. Dostupné také z: https://meraki.cisco.com/company/about.
3. *Remote Desktop Protocol*. TechTarget, 2017. Dostupné také z: https://searchenterprisedesktop.techtarget.com/definition/Remote-Desktop-Protocol-RDP.
4. *Client Details Page Overview*. Cisco Systems, Inc., 2018. Dostupné také z: https://documentation.meraki.com/zGeneral_Administration/Monitoring_and_Reporting/Client_Details_Page_Overview.
5. *CCNP Security Secure 642-637 Quick Reference: Cisco Layer 2 Security*. Cisco Press, 2011. Dostupné také z: https://www.ciscopress.com/articles/article.asp?p=1681033&seqNum=3.
6. *Supernetting and Classless Interdomain Routing*. Microsoft, 2012. Dostupné také z: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc958837(v=technet.10).
7. *VLANS for Meraki MX Appliances*. Performance Enhancements, Inc., 2019. Dostupné také z: https://www.pei.com/configure-vlans-meraki-mx/.
8. *Port Forwarding and NAT Rules on the MX*. Cisco Systems, Inc., 2018. Dostupné také z: https://documentation.meraki.com/MX/NAT_and_Port_Forwarding/Port_Forwarding_and_NAT_Rules_on_the_MX.
9. *Application-specific integrated circuit*. Wikimedia Foundation, Inc., 2020. Dostupné také z: https://en.wikipedia.org/wiki/Application-specific_integrated_circuit.
10. *Inter vlan on SG300-28PP L3*. pavlos82. Dostupné také z: https://community.cisco.com/t5/switching/inter-vlan-on-sg300-28pp-l3/td-p/3308201.
11. *Konfigurieren Sie HSRP in Cisco IOS Router*. FlatFeefsbo. Dostupné také z: https://flatfeefsbo.com/cisco/16-configure-hsrp-in-cisco-ios-router.html.
12. *Configuring RADIUS Authentication with WPA2-Enterprise*. Cisco Systems, Inc. Dostupné také z: https://documentation.meraki.com/MR/Encryption_and_Authentication/Configuring_RADIUS_Authentication_with_WPA2-Enterprise.
13. *Plan NPS as a RADIUS proxy*. Microsoft, 2020. Dostupné také z: https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-plan-proxy.

14. *Configuring RADIUS Authentication with a Sign-on Splash Page*. Cisco Systems, Inc., 2018. Dostupné také z: https://documentation.meraki.com/zGeneral_Administration/Cross-Platform_Content/Configuring_RADIUS_Authentication_with_a_Sign-on_Splash_Page.

15. *Cisco Spanning Tree Protocol Guide*. networkstraining.com. Dostupné také z: https://www.networkstraining.com/cisco-spanning-tree-protocol/.

16. *VirtualBox.org*. Dostupné také z: https://www.virtualbox.org/.

17. *How to Install macOS High Sierra in VirtualBox on Windows 10*. LifeSavvy Media, 2017. Dostupné také z: https://www.howtogeek.com/289594/how-to-install-macos-sierra-in-virtualbox-on-windows-10/.

18. *WinSCP Script Commands*. WinSCP.net, 2019. Dostupné také z: https://winscp.net/eng/docs/scriptcommand_option.